Lucent Technologies
Bell Labs Innovations

Several recipes for motherhood and apple pie

Brian K. Reid

Research director,

Bell Labs Silicon Valley

13 June 2000

Security is good

- We want to be secure.
- We will be careful.
- We will be diligent.
- We will not make mistakes.
- We will keep the bad people out of our computers.
- We will let only good people into our computers.
- We will be secure.

- Life will be excellent.

We don't have to worry…

- **We use the best firewall. We're safe.**
- **We use the strongest encryption available. We're safe.**
- **We have backups onsite and offsite. We're safe.**
- **We have no HR issues. Our employees are always perfectly happy. We're safe.**

What kind of security?

- National security
- Social security
- Physical security
- Emotional security
- Negotiable security
- Financial security
- Information security

- Internet security

What kind of security??

- National security
- Social security
- Physical security
- Emotional security
- Negotiable security
- Financial security
- Information security

- Internet security

What do these concepts have in common?

- **Stasis**
- **Comfort**
- **Control**
- **Impossibility**

You can run, but you can't hide. Absolute security is not only impossible, it's meaningless.

Security is feeling safe .

- National security
- Social security
- Physical security
- Emotional security
- Negotiable security
- Financial security
- Information security

- Internet security

One really good way to *feel* safe is to *be* safe.

Other techniques are cheaper and less intrusive.

Some are even possible.

A visit to the spin doctor

A conversation in northern New Mexico:

“Um, Sir, you know how that runaway forest fire destroyed our primary and secondary backup sites, and how all of our data was lost?”

“Yes.”

“Well, we just got a complete copy from China, and we’re back in business.”

Odds, not guarantees

.

- **Effective national security cannot guarantee that you will survive. Only that most people will.**

- **Financial security doesn't mean that you will never be desperate for money. Only that it's very unlikely.**

- **Emotional security doesn't mean that you will never be unhappy. Just that it won't ruin your life.**

- **Most people can't break in, and the ones that *can* will probably break into somebody else's.**

Security and publicity

If 10 million people live in a city

And one of them was mugged last year

Then you could say, honestly, that the city has good security

Unless the one who was mugged is the mayor’s child…

Or the newspaper editor’s child

(It would be true, but you couldn’t say it)

What's the point?

- Security isn't about technology
- It's about
  - Formal procedure
  - Recognizing the limitations of human beings
  - Publicity management
  - Risk management
  - Auditability
- These factors all enable you to be more confident that you have better security

But technology helps

- Technology enables vigilance
- Technology lets you automate something that you understand, so you can be more precise
  - (Example: LASIK)
- Technology increases your reach

Fortification is not security

- Strong barriers are nice
- But they are not enough. Security requires vigilance and flexibility more than fortification
- (Remember the Maginot line?)
- Vigilance requires training, cleverness, alertness, and experience

All power tools can kill

.

- Power tools enable a trained person to do a job better
- Any power tool can be misused
- The more power the tool has, the more damage it can cause if misused
- Security tools are no exception to this rule
- But it takes more expertise to see damage caused by a firewall than by a chainsaw

Step 1: the official nightmare

What is it, exactly, that you are afraid of:

- **Data leaving your facility without authorization?**
- **Data *entering* your facility without authorization?**
- **Data missing?**
- **Data damaged or altered, visibly or invisibly?**
- **Authorized changes, but untraceable?**
- **Fraudulent transactions?**

- **Publicity claiming that any of the above have happened, whether it is true or not?**

Nightmare examples 1

Unauthorized exit: most common nightmare

- **Medical history**
- **Trade secrets**
- **Political plans**
- **Personal information**

Nightmare examples 2

Unauthorized entry of data

- Real estate or financial data
- Degrees or education achieved
- Birth records for citizenship
- First claim date

Nightmare examples 3

Missing data

- Criminal record or motor vehicle history
- Real estate ownership
- Vital statistics: you were never born

Step 2: quantifying risk

What is the cost (and to whom) of failure?

- **Bad reputation?**
- **Injury or death?**
- **Loss of money?**
- **Small loss to many people, not major to any of them?**
- **Catastrophic loss to some?**
- **Loss of public confidence?**

Measuring cost

.

- In banking, we assume reversibility
- Money can be put back
- Many situations are not reversible:
  - Elections
  - Damaged reputations
  - Computerized medical procedures
- Cost measurement in irreversible situation is much harder

Step 3: think about a solution

- **Now that you have quantified the risk, evaluate the cost of a solution**
- **Compare it with the cost of not having a solution.**
- **Sometimes the right answer is to do nothing.**
- **Sometimes that is a very wrong answer.**

Story: Allentown telephones

- **A company once manufactured telephones in Pennsylvania**
- **Their bookkeeper told them that phones were being stolen**
- **They sought advice from a security expert, and from an accountant**
- **The conclusion….**

Loss rate limits

- We can assume that each corrupt employee can steal no more than one telephone per day
- To steal a telephone you must somehow carry it out of the factory
- To steal data you need do no such thing. We can make no assumptions about the amount of data one corrupt employee can steal in a day

Cyber people are invisible .

- Physical crimes (theft, vandalism, forgery, extortion, etc) must obey the laws of nature.
- Did children stop believing in Santa Claus when they were old enough to compute that he would have to fly faster than the speed of light?
- Cyber crimes do not need to obey the laws of nature. A cyber vandal really *can* be everywhere at once.

Don’t ever admit it, but .

- In the physical world, a small amount of fraudulent activity is inevitable.
- We assume that the amount is small because we would see evidence if it started to get large.
- In the online world, where things are invisible, we cannot have the comfort of trusting our 5 senses.

Identity and authentication

Our activities require various levels of authentication:

- A trip to the local bank
- A trip to a private Swiss bank
- Voting
- Joining your spouse behind closed doors

Any activity that can be performed online also needs authentication

Wait a minute…

- The solution depends on ability to:
  - Identify people or their actions
  - Record what happens
  - Audit it
  - Monitor to look for unexpected events
  - Ensure that fraud and failure in automated system is within expectations
- This requires authentication

Strong authentication

- **Today’s state of the art in authentication:**
  - **You must have something**
  - **And you must know something**
  - **To authenticate, verify that they have the object and know the secret**
- **“Have” requirement: can’t share**
- **“Know” requirement: can’t steal**
- **But you’ve all seen “Gattica”, right?**

Here the apples get sour .

- **Tradition in the USA: people can have the right to be anonymous**
- **Federal legislation in the 1960's forbade the use of strong authentication for voting**
- **In fighting cyber crime, strong authentication is very important**
- **Instant conflict between old traditions and new needs**

Perfect security?

.

- **Perfect for whom?**
- **Literature has tales of a future where government controls everything in the name of security**
- **This is why, in our country, the military is not in charge**
- **Democracy requires checks and balances. Here we balance need for security against need for anonymity**

Security and privacy

.

- **We all agree that security and privacy are excellent ingredients for apple pie**
- **What happens when *your* need for security…**
- **Interferes with *my* need for privacy?**
- **What happens if state security requires that citizens have no privacy?**
- **What happens if citizens' privacy endangers state security?**

The challenge for technologists .

- Never forget that technology is a tool, not a goal in itself
- Even though it's fun, lucrative, and makes the whole world envious of California
- Recognize that the political and social agenda must always dominate the technical agenda
- Though wealth, from technology, can influence the agenda

The challenge for executives .

- Needs of information security will always conflict with principles of privacy and anonymity
- Design and implementation of security procedures always requires educated compromise
- We technologists can talk about best practices, but executives must do final balance
- Political risks are always the greatest

Lucent Technologies
Bell Labs Innovations

Thank you for your attention

Brian K. Reid, PhD

Research director,

Bell Labs Silicon Valley

13 June 2000

**Bell Labs is the innovation arm of Lucent Technologies
and, historically,
of much of the technological world**

http://pa.bell-labs.com/~bkreid/13june2000.ppt